CHAPTER 8

CLEARANCE

8-1 BASIC POLICY

1. The Department of the Navy Central Adjudication Facility (DON CAF) is designated by the Secretary of the Navy as the single clearance granting authority for the Department of the Navy. The DON CAF issues final security clearances for civilian and military personnel at the request of DON commands and activities, upon affirmation that granting the clearance is clearly consistent with the interests of national security. Once issued, a security clearance remains valid provided the cleared individual continues compliance with personnel security standards and has no subsequent break in service exceeding 24 months.

2. A security clearance is not a de facto authorization for an individual to access classified information. Authorization to access classified information is a separate command level determination dependent on whether an individual who has the requisite security clearance also has a need for access to classified information in the performance of official duties. Access to Sensitive Compartmented Information (SCI) is a separate issue addressed in chapter 9.

3. The DON CAF determines the security clearance for DON personnel using the appendix G adjudicative guidelines to assess the loyalty, reliability and trustworthiness issues documented in personnel security investigations. Security clearance is initially issued upon adjudication of the prerequisite security investigation, and is reestablished upon adjudication of subsequent investigation(s). Certification is provided to a command when a clearance is required to support local access determinations. **Security clearance will be established at the highest level supportable by the prerequisite security investigation.***

*** For the purpose of this regulation the terms "security clearance" and "security clearance eligibility" will be synonymous.**

8-2 RECIPROCAL ACCEPTANCE OF SECURITY CLEARANCES

1. A security clearance determination by an approved agency of the Federal Government will be mutually and reciprocally accepted throughout the Federal Government provided the following

conditions are met: (1) there is no break in continuous government service greater than 24 months; (2) the investigative basis is adequate for the clearance to be granted, and (3) no new derogatory information is identified. The security clearance will be verified by the cognizant CAF, without additional adjudication.

2. A denial or revocation of security clearance eligibility may also be reciprocally accepted by agencies of the Federal Government. However, if the denial or revocation determination was made more than 12 months prior and a new clearance eligibility determination is requested, the new request will be processed in accordance with the reconsideration procedures provided in chapter 10.

3. **Continuous service** for security clearance eligibility purposes is active duty military service (including attendance at the military academies); active status in the military reserve, National Guard, NROTC, active Individual Ready Reserves (IRR), etc.; civilian employment in the Federal Government; employment with a DoD contractor that involves a security clearance under the National Industrial Security Program (NISP) or, a combination of these. Continuous service is maintained with a change from one status to another as long as there is no break greater than 24 months. Retired status does not qualify as **continuous service.**

4. Security clearance eligibility established within DoD will be accepted by the Department of Energy (DOE) and Nuclear Regulatory Commission (NRC) as the basis for access to Restricted Data of the same or lower classification. DOE and NRC clearance determinations are accepted by DoD as follows:

DOE and NRC Clearances	**DoD Clearance Eligibility**
"L" (For NRC employees, consultant personnel, and for DOE contractor personnel only, access up to Secret except Restricted Data for which access to Confidential only is authorized.)	Secret
"Q"	Secret
"Q" (specifying Top Secret access)	Top Secret

5. Security clearances granted conditionally (and SCI access eligibility established as an exception) are not bound by the reciprocity requirements.

8-3 CLEARANCE PROHIBITIONS

1. Only United States citizens who are either members of the executive branch of the U.S. Government or employees of contractors under the National Industrial Security Program (NISP) are eligible for security clearance. Occasionally, it is necessary for the DON to authorize access for persons not meeting these requirements; paragraph 9-14 governs these situations.

2. When this regulation refers to U.S. citizens, it makes no distinction between those who are U.S. citizens by birth, those who are U.S. nationals, those who have derived U.S. citizenship or those who acquired it through naturalization. For the purpose of issuance of a security clearance, citizens of the Federated States of Micronesia (FSM) and the Republic of the Marshall Islands are considered U.S. citizens. Appendix I provides guidance on validating U.S. citizenship.

3. A security clearance will not be granted for:

a. Persons in nonsensitive civilian positions;

b. Persons (such as guards and emergency service personnel) who may only have inadvertent access to sensitive information or areas;

c. Persons (such as maintenance, food services, or cleaning personnel) who perform unclassified duties within a restricted or controlled area, or other area where classified information may be present, unless access to classified information or materials cannot be reasonably prevented;

d. Persons (such as vendors and other commercial sales or service personnel) who do not require access to classified information and whose access to classified information can be prevented by a cleared escort.

4. The Facility Access Determination (FAD) program is used for trustworthiness determinations for contractor personnel when no access to classified information is required (paragraph 7-6 applies).

5. Elected members of Congress are not processed for security clearance eligibility. They may be granted access to classified information as required for the performance of their duties. Procedures for visits by elected members of Congress requiring access to classified information are provided in paragraph 11-4. Members of congressional staffs may be processed for security

clearance eligibility, as necessary, through the Security Division, Washington Headquarters Services, Department of Defense in accordance with DoD Directive 5142.1, Assistant Secretary of Defense (Legislative Affairs), 2 Jul 82 (NOTAL).

6. State governors are not processed for security clearance eligibility. Commanding officers may grant access to specifically designated classified information to these individuals, on a "**need to know**" basis, when approved by CNO (N09N2). Staff personnel of the governor's office who require access to DON classified information are investigated and cleared by the DON CAF, as appropriate.

7. Members of the U.S. Supreme Court, the Federal judiciary and the Supreme Courts of the individual states are not processed for security clearance eligibility. They may be granted access to classified information to the extent necessary to adjudicate assigned cases. For SCI, access may be granted upon concurrence from COMNAVSECGRU or SSO Navy.

8-4 RECORDING DETERMINATIONS

1. The Navy Joint Adjudication and Clearance System (NJACS) is the official central repository for DON personnel security determination records and includes clearance, access and investigative data. NJACS data supports management of the DON personnel security program, central management of the reinvestigation program, budget management requirements and congressional reporting requirements.

2. The DON CAF is charged with maintaining the NJACS data. Every security clearance determination made at the DON CAF is recorded in the NJACS. Initial access determinations are recorded in the NJACS. Investigative data forwarded from the Defense Security Service (DSS) and the US Investigative Service (USIS) is included in the NJACS. NJACS personnel security data codes are found in exhibit 8A.

3. The DON CAF formally certifies security clearance determinations to requesting commands. The DON CAF's certification is generated using NJACS data and provides commands with the documentation required to support local access determinations and other local program management requirements. Because the DON CAF certification supports command access determinations, it must be maintained in the individual's local service record or official personnel file until the individual separates, the individual's security clearance is revoked or until the certification is replaced by a more current record. **Copies** of the DON CAF certification may additionally be

maintained in local security files. The Marine Corps Total Force System (MCTFS) will provide the security clearance certification for Marine Corps military members.

4. The personnel security record maintained in the NJACS database is processed through tape transfers into the DON personnel data systems to include the Officer Distribution Control Report (ODCR), Enlisted Distribution Verification Report (EDVR), Marine Corps Total Force System (MCTFS) and the Defense Civilian Personnel Data System (DCPDS). NJACS data is also reflected on transfer orders. These sources of NJACS data may be used temporarily to support local access determinations when the DON CAF security clearance certification is not found in the individual's service record or official personnel file, pending receipt of a replacement for the DON CAF certification record. In these cases, commands will submit an OPNAV 5510/413 to the DON CAF requesting a security clearance determination. The DON CAF will forward a replacement certification. Procedures for temporary access determinations are found in paragraph 9-7.

5. Additionally, information maintained in the NJACS is electronically entered into the Defense Clearance and Investigations Index (DCII) discussed in appendix E. Commands with DCII access may use DCII data records in lieu of the DON CAF certification records, as appropriate, to support local access determinations.

6. Once issued, the DON CAF security clearance certification remains valid provided the individual continues compliance with personnel security standards and has no subsequent break in service exceeding 24 months. (A change in commands or duties is not a "break in service.")

7. Commands will keep local access records. Paragraph 9-5 addresses access recording requirements.

8-5 INTERIM SECURITY CLEARANCE

1. Commands may grant interim security clearance and access (except for SCI access) pending completion of full investigative requirements and pending establishment of a final security clearance by the DON CAF. Interim clearances are granted, by authority delegated by the Director, DON CAF to the commanding officer under the following conditions:

a. Interim Top Secret security clearance.

(1) The existence of a favorable investigation (e.g. ENTNAC, NAC, NACI, etc., (paragraph 6-2 applies);

(2) A favorable review of the completed personnel security questionnaire (PSQ);

(3) The submission of the SSBI request to DSS; and

(4) A favorable review of local records, as defined in paragraph 6-12.

b. Interim Secret or Confidential security clearance.

(1) A favorable review of investigative request questionnaire;

(2) The submission of an appropriate investigative request to the investigative agency (paragraph 6-14 applies); and

(3) A favorable review of local records (paragraph 6-12 applies).

2. Commands will record interim security clearance actions using OPNAV 5510/413, Personnel Security Action Request, Part III under item 15. Item 22 of OPNAV 5510/413 will reflect the date and type of investigation requested. The interim clearance will be granted by signature of the commanding officer or designee who has been the subject of a favorably completed Single Scope Background Investigation (SSBI). The OPNAV 5510/413 will NOT be forwarded to the DON CAF at this time, but will be held until follow-up action is necessary.

3. It is important to ensure that the request for investigation submitted to support a required final security clearance reaches its destination, especially when interim clearances are granted. Commands that do not use the EPSQ to submit requests electronically, are strongly encouraged to use registered or certified mail for these specific requests so that receipt may be confirmed.

4. If a receipt confirming final clearance is not received within 180 days of submission of the request for investigation, a copy of the OPNAV 5510/413 recording the interim clearance will be boldly marked "TRACER" in item 22 and will be forwarded to the DON CAF. The DON CAF will respond to these tracers within 30 days.

5. The interim clearance may not be continued in excess of 1 year without a current confirmation from the DON CAF that the investigation contains no disqualifying information.

6. When the command receives a Letter of Intent (LOI) from the DON CAF to deny an individual's security clearance, the commanding officer will withdraw any interim security clearances issued and associated access will be suspended. Procedures for suspending access are found in paragraph 9-18.

8-6 GRANTING A SECURITY CLEARANCE

1. The DON CAF is the sole DON security clearance granting authority. The DON CAF adjudicates investigations at the highest level supportable by the completed prerequisite investigation. Investigative requirements are outlined in chapter 6.

2. When it is determined that an individual will require access to classified information to perform assigned duties, commands will review the individual's service record or official personnel folder to ensure the individual has the necessary security clearance certification. (Commands with DCII access will search DCII data to determine clearance eligibility.)

a. When the individual does not have the appropriate security clearance certification, but local records indicate the appropriate investigation exists, the command will submit an OPNAV 5510/413 request to the DON CAF to obtain the required certification. (Commands with DCII access need not request the DON CAF certification, DCII data will suffice.)

b. When the individual has neither the required clearance nor the required investigation to support the security clearance determination, the command will submit the appropriate request for investigation. Upon completion, the investigation will go to the DON CAF where a clearance determination will be made and the requesting command will be subsequently notified. Interim security clearance procedures may be employed as necessary.

8-7 UNIQUE SECURITY CLEARANCE REQUIREMENTS

1. Commanding Officer Clearance. Every commanding officer must have a favorably adjudicated SSBI and the security clearance equivalent to the highest level of classified information maintained at the command. The incumbent commanding officer will review the records of the prospective commanding officer to ensure that the individual has the necessary investigation and security clearance certification to assume command. In the

absence of an incumbent commanding officer, the next senior in the chain of command will ensure the records are reviewed. When the prospective commanding officer does not have the appropriate security clearance certification or SSBI, the incumbent commanding officer will ensure the necessary requests for certification and/or investigation are submitted.

2. Cryptographic Duties. Commands cannot grant interim security clearances for cryptographic duties. Clearance eligibility must be established by the DON CAF before access is allowed to U.S. cryptographic information.

3. Reserve Personnel. Navy and Marine Corps reserve personnel in an **"active status"** are considered to have continuous service and may be granted access as necessary and supportable by the DON CAF security clearance certification.

4. Individual Ready Reserves (IRR). IRR members will have security clearance established by the DON CAF as necessary. All due process procedures will be afforded IRR members nominated for security clearance.

5. Rating/Military Operations Specialty (MOS) Requirements. To maintain mobility and operational readiness, the Chief of Naval Personnel (Pers-831) or Headquarters Marine Corps (HQMC) may require individuals in specified ratings/MOS to have security clearance (eligibility) established by the DON CAF to support subsequent assignments.

a. Commands will use the continuous evaluation process to maintain security clearance (eligibility) for these specified ratings/MOS. PR's are not required unless the conditions outlined in paragraph 6-2.2g also exist.

b. Commands will forward potentially disqualifying information to the DON CAF for determination of continued eligibility for security clearance.

6. Personnel Assigned to Other Federal Agencies. The DON CAF will establish and provide certification of security clearance eligibility for DON employees assigned to other Federal agencies.

7. Access by Consultants to Government Contracting Activities (GCA). A consultant who is hired by a GCA and will only require access to classified information at a GCA activity or in connection with authorized visits, is not processed for a security clearance under the National Industrial Security Program (NISP). The consultant is considered an employee of the GCA for

security clearance and access purposes and will be adjudicated for security clearance by the DON CAF.

8-8 CLEARANCE UNDER THE NATIONAL INDUSTRIAL SECURITY PROGRAM (NISP)

1. Employees of contractors granted facility clearances under the NISP may be granted personnel security clearances when there is a bona fide requirement to access classified information in connection with performance on a classified contract or R&D program. Contractor personnel security investigations are conducted by the Defense Security Service (DSS). Investigative results are then adjudicated and security clearance eligibility is established by the DSS Operations Center, Columbus (OCC).

2. Employees of contractors requiring access to SCI under the auspices of the DON are adjudicated for SCI access eligibility by the DON CAF. After adjudication of SCI access eligibility, the investigative results are forwarded to DSS OCC for security clearance adjudication.

3. Under previous policy, contractors were delegated authority to act on behalf of the DoD to grant Confidential clearances to qualified employees. This authority has been rescinded. However, contractor-granted clearances granted to employees prior to January 1991, unaffected by upgrade or administrative withdrawal, remain valid.

4. Interim Secret or Confidential security clearances may be granted to eligible contractor employees by DSS OCC on a temporary basis pending completion of a personnel security investigation.

5. Interim Top Secret security clearances may be granted to eligible contractor employees by DSS OCC based on approval from the contracting command or activity. DON contracting commands in receipt of requests for interim Top Secret security clearances will validate the contract, contractor need to know, and necessity for the interim clearance.

6. Commanding officers will report to DSS OCC any adverse or questionable information which comes to their attention concerning a cleared contractor employee assigned to a worksite under their control. An information copy of the report will also be forwarded to the Defense Security Service (DSS) Operating Location Office (OPLOC) identified on the Contract Security Classification Specificiation (DD Form 254). A sample DD 254 is at exhibit 11A of reference (d). Commanding officers will also

report adverse or questionable information to the DON CAF when a cleared contractor employee has SCI access.

7. Commands are responsible to ensure all clearance and access requirements are identified on the DD 254. Command procedures for granting or denying access to classified information for cleared contractor employees is provided in paragraph 9-13.

8-9 CLEARANCE WITHDRAWAL OR ADJUSTMENT

1. Access terminates when an individual transfers from one command another, however clearance requirements will normally remain unaffected. Commands will debrief individuals who are transferring to another command as outlined in paragraph 4-11, but execution of a Security Termination Statement is not required. Commands will make every effort to ensure that the DON CAF security clearance certification is properly filed in the service record or official personnel folder and forwarded to the individuals new command to support future access determinations.

2. Commanding officers will administratively withdraw an individual's access when a permanent change in official duties (i.e. rating/MOS changes) eliminates the requirement for security clearance and access. The command will debrief the individual as outlined in paragraph 4-11 and file the executed Security Termination Statement in the individual's service record or official personnel folder. Commands will notify the DON CAF using OPNAV 5510/413 that the individual no longer requires clearance and access. The DON CAF will adjust the NJACS accordingly.

3. When the level of access required for an individual's official duties changes, the command will adjust the authorized access accordingly, providing the new requirement does not exceed the level allowed by the security clearance. If the level of access required will exceed the level allowed by the DON CAF security clearance certification, commands will ensure the appropriate investigation is requested and may consider granting an interim clearance as specified in paragraph 8-5.

4. The administrative withdrawal or downgrading of a security clearance or access is not authorized when prompted by developed derogatory information. The command may **suspend** the individual's access for cause, and must report the suspension and/or the derogatory information to the DON CAF. The suspension of access must be accomplished in accordance with paragraph 9-18. (When SCI access is at issue the command Special Security Officer will coordinate the action.) A command report of suspension of access for cause will automatically result in the DON CAF suspension of

the individual's security clearance. The clearance certification will be removed from local records. Once security clearance is suspended by the DON CAF, the individual may not be granted access unless the security clearance is reestablished by the DON CAF.

5. **Transfer in Status (TIS).** The TIS is a process in which an individual may be transferred from one DoD component, command, or activity, to another DoD component, command, or activity in an SCI indoctrinated status. TIS should not be confused with the process of individual's transferring with established security clearance eligibility. Chapter 9 provides additional guidance concerning SCI access.

8-10 DENIAL OR REVOCATION OF SECURITY CLEARANCE

1. Once the DON CAF grants a security clearance it remains valid provided the individual continues compliance with personnel security standards and has no subsequent break in service exceeding 24 months. Commands are ultimately responsible for ensuring that the DON CAF is apprised accordingly when either of these invalidating factors exist. To satisfy this requirement, commands must implement a proactive continuous evaluation program as described in chapter 10. Whenever information develops that suggests an individual may no longer be in compliance with personnel security standards, commands must report the issues to the DON CAF for adjudication using the OPNAV 5510/413. For SCI, refer to reference (c) for reporting requirements. Exhibit 10A provides a checklist of issues that must be reported.

2. In the event the DON CAF determines that an individual either fails or ceases to meet the standards for security clearance, the DON CAF will begin the unfavorable determination process explained in paragraph 7-8. If the DON CAF determines a reported issue does not impact on the individuals security clearance, a security clearance certification will be reissued to the command.

3. Once the DON CAF makes a final unfavorable decision concerning an individual's security clearance, the command must remove all accesses authorized, and debrief the individual in accordance with paragraph 4-11, including execution of a Security Termination Statement even if the individual is appealing the unfavorable DON CAF decision. All previous clearance certificates will be removed and replaced with the LON.

8-11 REESTABLISHING A SECURITY CLEARANCE AFTER A DENIAL OR REVOCATION

1. Following an unfavorable security determination by the DON CAF, a request to reestablish security clearance may be submitted after a reasonable passage of time, normally a minimum of 12 months, when it is determined that the individual appears to meet the appendix G guidelines. Commands shall provide documentation to support the reestablishment of security clearance eligibility.

2. Interim security clearance and/or access and assignment to sensitive civilian positions is **not** authorized for individuals who have received an unfavorable determination until the DON CAF reestablishes the security clearance. If a favorable determination is not possible, the DON CAF will provide the commanding officer with specific reasons for upholding their previous decision.

EXHIBIT 8A

PERSONNEL SECURITY DATA CODES

1. SECURITY INVESTIGATIONS. Identifies the most recent Personnel Security Investigation (PSI) completed on an individual.

Code	PSI
1	Entrance National Agency Check (ENTNAC)
2	National Agency Check (NAC)
3	NAC plus Written Inquiries (NACI)
4	Background Investigation (BI)
5	Special Background Investigation (SBI)
6	NAC plus 10 years of service (obsolete)
7	NAC plus Special Investigative Inquiry (SII)
8	ENTNAC plus SII
9	Interview oriented BI (IBI)
A	Expanded NAC
B	Local Records Check (LRC) plus NACI requested
C	NACI requested
D	NAC or NACI plus BI or IBI requested
E	NAC plus SBI requested
F	BI/IBI (10-year scope)
G	Periodic Reinvestigation (PR) or BI/IBI
H	NAC plus partial SBI
I	Character Investigation (IRS)
J	PR
K	Limited BI (LBI) (OPM)
L	Minimum BI (MBI) (OPM)
M	SBI plus current NAC
N	NACI plus current NAC
O	SII
P	IBI/BI plus current NAC
Q	MBI plus current NAC
R	LBI plus current NAC
S	SBI plus current BI/IBI
T	IBI/BI requested
U	Other
V	SBI requested
W	LRC
X	MBI expanded
Y	LBI expanded
Z	NACI plus SII
#	Secret PR

2. SECURITY ELIGIBILITY. Provides the level of clearance eligibility established for an individual.

A	No clearance - Investigation reopened
B	SCI denied - Ineligible for clearance
C	Confidential
D	Clearance denied
E	Interim Confidential
F	SCI revoked - Ineligible for clearance
G	Secret - SCI denied
H	Secret - SCI revoked
I	Clearance pending - Investigation reopened
J	No Clearance Required - File created
K	Eligible for SCI w/waiver
L	Restricted to nonsensitive duties/not eligible
M	Top Secret only - SCI revoked
N	Top Secret only - SCI denied
O	Interim Secret
P	Interim Top Secret
Q	*No clearance/access required - favorable investigation*
R	Clearance revoked
S	Secret
T	Top Secret
U	Interim SCI
V	Top Secret - SCI Eligible
W	Top Secret - SCI requires adjudication
X	Action pending
Y	Pending adjudication/access suspended
Z	Adjudication action incomplete due to loss of jurisdiction
1	LAA Confidential
2	LAA Secret
3	Pending reply to Letter of Intent (LOI)/Statement of Reason (SOR)
4	Clearance administratively withdrawn
5	Position of trust (no clearance determination)
6	SCI denied (no clearance determination)
7	SCI revoked (no clearance determination)

3. CURRENT CLEARANCE/ACCESS AUTHORIZED. Indicates the actual clearance/access currently held by the individual.

A	No clearance - Investigation reopened
B	SCI denied - Ineligible for clearance
C	Confidential
D	Clearance denied
E	Interim Confidential
F	SCI revoked - Ineligible for clearance

G	Secret - SCI denied
H	Secret - SCI revoked
I	Clearance pending - Investigation reopened
J	No Clearance Required - File created
K	Eligible for SCI w/waiver
L	Restricted to nonsensitive duties/not eligible for sensitive duties
M	Top Secret only - SCI revoked
N	Top Secret only - SCI denied
O	Interim Secret
P	Interim Top Secret
Q	No clearance/access required - favorable investigation
R	Clearance revoked
S	Secret
T	Top Secret
U	Interim SCI
V	DCID 1/14 Eligible
W	Top Secret - SCI requires adjudication
X	Action pending
Y	Pending adjudication/access suspended
Z	Adjudicative action incomplete due to loss of jurisdiction
1	LAA Confidential
2	LAA Secret
3	Pending reply to Letter of Intent (LOI)/Statement of Reasons (SOR)
4	Clearance administratively withdrawn
5	Position of trust (no clearance required)
6	SCI denied (no clearance determination)
7	SCI revoked (no clearance determination)